Cybersecurity for information professionals: The organisational dimension

Matt Moore and Kelly Tall*

This article focuses on the organisational aspects of cybersecurity. We begin by identifying potential hostile parties and the methods they use to penetrate systems. Outlining the NIST Cybersecurity Framework, we discuss the responses to cybersecurity issues by information professionals and their role in this environment.

INTRODUCTION

Our previous article on cybersecurity approached the issue from the perspective of the individual internet user and showed the breadth of issues that we face and the simple things we can do to make our online interactions safer. This article has a different focus: How are organisations managing the cybersecurity risks that they face?

All Australians have some kind of relationship with large organisations that hold their data, be they corporations, not-for-profits, or governments. While we can take efforts to personally safeguard our own data, we are also reliant on the efforts of others. As consumers and citizens, we often blithely assume that these organisations are protecting their (our) data from harm. Those assumptions may not be wholly justified. This article will begin with an overview of the types of hostile parties and threats that organisations face and how they are meeting those threats.

The situation becomes even more complex when we are employed in roles where we play a role in information security – which we often do as information professionals. "Security" may not be our main priority but it is nevertheless there. The second half of the article, through practitioner quotes and academic research, explores the challenges that managing security as one of a number of information priorities presents to us.

WHO ARE THE HOSTILE PARTIES?

While the recent news has been full of hackers and rogue states like North Korea engaging in cyber attacks, many of the actual threats may be closer to home. Surveys by PwC[1] and EY[2] indicate that the most likely sources of data breaches are past or current employers and contractors. Edward Snowden and Bradley Manning are perhaps the best known individuals of this type but they are relatively rare in that their activities have gone public. Many internal incidents are kept from the public: 75% of respondents to the PwC survey said they did not involve law enforcement in internal breaches. The Snowden and Manning breaches are interesting in that their perpetrators were not primarily motivated by financial gain. They also highlight the security vs sharing dilemma. Following 9/11, there was a push within the US intelligence community to share information as the lack of such collaboration was seen as a contributing factor to the failure to prevent the attacks. Both individuals had access to large volumes of information, far more than needed to do their specific jobs. At the same time, millions of government employees and contractors had access to confidential, secret or top secret information and

* Matt Moore has spent 15 years working in knowledge and information management, learning and development and internal communications with organisations such as IBM, Oracle and the Australian Securities and Investments Commission. He lectures at the University of Technology Sydney and is a former chair of the New South Wales Knowledge Management Forum. Kelly Tall is an experienced market researcher with a passion for data visualisation. She has worked with many well-known global and Australian brands. All websites viewed June 2015.

[1] PricewaterhouseCoopers. *The 2015 Global State of Information Security Survey* (2015) http://www.pwc.com.au/consulting/publications/global-information-security/index.htm.

[2] Ernst & Young, *Global Information Security Survey* (2014) http://www.ey.com/GL/en/Services/Advisory/EY-global-information-security-survey-2014.

do not seem to have leaked it.[3] Of course, we can never know, but anecdotally employee breaches are a long-tail threat: they are rare but when they happen, they can be catastrophic.

External threats include criminal syndicates, commercial competitors and foreign nation states. In some respects these entities are easy to understand. While their lines of attack may be unpredictable, what they want is simple: commercial advantage. This may take the form of outright fraud or financial theft, or it may be that intellectual property is the target. The technical resources that these entities have at their disposal are formidable and the internet is not a well-policed place. Despite the slick facades of corporate websites, it remains more like a wild west frontier saloon than an inner city coffee shop.

Taking this lawless theme further is the network of individuals and groups that the media label "hackers". These people may be in the pay of gangs or foreign states, or they may be simply trying to get into systems for fun and bragging rights, or they may have some kind of ideological animus against their targets. Their range of motives and fluid-to-non-existent organisation makes them very hard to track and predict.

We also have an incomplete understanding of the extent to which domestic intelligence agencies are spying on us. The never-ending "war on terror" has been a pretext for ever greater levels of state surveillance (eg mandatory data retention). While some government surveillance is necessary, the lack of public scrutiny these activities have received is worrying. Intelligence agencies will always ask for expanded powers but they should not necessarily be afforded them.

WHAT TECHNIQUES ARE USED?

CERT Australia (Computer Emergency Response Team) is an agency, within the Australian Federal Attorney General's Department, with a focus on cybercrime. Their 2013 survey indicated that the main incidents that Australian businesses had faced in the previous 12 months were:

- Targeted "spear phishing" emails, ie emails with web links that appear to be from trusted source but actually lead to a compromised environment.
- Viruses, worms, trojans or rootkits: various unpleasant bits of code that can be introduced into systems by email, the web, or USB devices.
- Theft of mobile devices: plain, old-fashioned stealing.
- Unauthorised access: finding gaps in security.
- Distributed denial of service: the use of compromised networks of devices that bring down websites by trying to access these sites en masse.[4]

Some of these attacks can be remarkably sophisticated, with their perpetrators gradually gaining access to systems by targeting the movements of specific individuals from an organisation over time and building up a presence within an organisation's IT system, whereas others can be crude and opportunistic. Not every criminal is a mastermind.

One concept that is useful here is the "attack surface". This is the sum of the different points of potential attack across a network. Unused functionality that is switched on increases the attack surface. Multiple and overlapping systems increase the attack surface. Hardware entry points (eg USBs) increase the attack surface. Allowing more people to access your information increases the attack surface. Reducing an attack surface does not mean removing useful functionality or preventing people from doing their jobs – but it does provide another reason to remove unnecessary infrastructure.

THE RESPONSE TO CYBERSECURITY THREATS: THE NIST CYBERSECURITY FRAMEWORK

How have governments and industry responded to these threats? In 2014, a US federal government agency called the National Institute of Standards and Technology (NIST) issued a voluntary

[3] Aftergood S, "Number of Security Clearances Soars" *Federation of American Scientists – Secrecy News blog* (20 September 2011) http://fas.org/blogs/secrecy/2011/09/clearances.

[4] CERT Australia, *Cyber Crime and Security Survey 2013* (2013) https://www.cert.gov.au/newsroom.

framework for organisations to manage cybersecurity risks.[5] While voluntary, this framework has become the de facto standard for institutional cybersecurity in both the public and private sectors in the US and overseas. It should be noted that there are other information security frameworks such as ISO 27001:2013 that are in use. While the frameworks may appear different, they have many overlapping elements. One advantage of the NIST framework is that it is free.

The framework consists of a core, tiers and profiles. The core is a set of functions, categories, subcategories and informative references that map out the different activities required to manage cybersecurity risks effectively. The functions and categories are listed below to give readers a sense of the scope of activities that organisations need to undertake.

TABLE 1 NIST Cybersecurity Framework: Core functions and categories

Function	Category
Identify	Asset Management. The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
	Business Environment. The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Governance. The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Risk Assessment. The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management Strategy. The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
Protect	Access Control. Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
	Awareness and Training. The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security. Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Information Protection Processes and Procedures. Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance. Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
	Protective Technology. Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Detect	Anomalies and Events. Anomalous activity is detected in a timely manner and the potential impact of events is understood.
	Security Continuous Monitoring. The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes. Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

[5] US National Institute of Standards and Technology, *Cybersecurity Framework* (2014) http://www.nist.gov/cyberframework.

TABLE 1 *continued*

Function	Category
Respond	Response Planning. Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
	Communications. Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
	Analysis (eg Data Forensics). Analysis is conducted to ensure adequate response and support recovery activities.
	Mitigation. Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
	Improvements. Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
Recover	Recovery Planning. Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
	Improvements. Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications (eg Public Relations). Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Under the function "Identify" and the category "Asset Management", there are six sub-categories, the first of which is "ID.AM-1: Physical devices and systems within the organization are inventoried". Associated with this sub-category are a set references to provide further information and support: CCS CSC 1; COBIT 5 BAI09.01, BAI09.02; ISA 62443-2-1:2009 4.2.3.4; ISA 62443-3-3:2013 SR 7.8; ISO/IEC 27001:2013 A.8.1.1, A.8.1.2; NIST SP 800-53 Rev. 4 CM-8.

The tiers refer to the extent to which the organisation can undertake a certain category. They are: Partial; Risk Informed; Repeatable; and Adaptive. Not all organisations can and should be adaptive at all activities. The Profiles element of the framework allows an organisation to map their current position and their target state against the core and the tiers. Where they are gaps, they need to invest in building capability. However they may also be over-invested in certain activities.

The framework highlights a few key cybersecurity issues:

- Prevention is better than cure. "Identify" and "Protect" have significant weight in the framework because while prevention might be expensive, remediation after a breach can be even more expensive. The problem with getting management attention for prevention strategies is that:
  - Prevention begins with understanding what you have. This may sound basic but many organisations do not have a comprehensive picture of their network, hardware and software assets. Old assets are not necessarily decommissioned when something new comes and may hang around for years. Assets are not necessarily documented and those with the knowledge in their heads may move on. Many system breaches do not begin with the core systems, rather they target legacy devices or systems on the periphery of the network.
  - Complete prevention is impossible so you need to be constantly monitoring. A completely secure system is very difficult and very expensive to achieve – and security is often inversely proportional to the system's accessibility (and therefore usefulness). Monitoring can be thought of as installing a burglar alarm as opposed to an electric fence.
  - Once you have identified a threat, you need to know what to do next. If some form of incursion is likely (and it is likely), you need to have a plan as to how you will deal with it.

INFORMATION PROFESSIONALS AND CYBERSECURITY

Cybersecurity tends to generate a range of views across the information management practitioner and research community. On the one hand, most knowledge and information managers are not

cybersecurity professionals. While some do operate as gatekeepers, most are tasked with enabling people to share their information rather than hide it. One resulting perspective is that information professionals do not take cybersecurity seriously.

Academics Murray Jennix and Alexandra Durcikova explored the relationship between knowledge management and information security via a literature review, practitioner survey and job listings analysis:

> While the findings in the KM research literature were better than expected, the findings in KM practitioner job postings were as expected, and to a degree disappointing. The findings reflect that KM practitioners still totally focus on knowledge capture, storage and sharing and that Information Security is an afterthought. Only just over 10% of the non-defense related job postings had requirements for understanding organizational security standards or policies and only two KM technician postings requested Information Security certifications. The survey results mimic this suggesting that the focus is on capturing and sharing knowledge and much less focus is paid on security access to knowledge. Organizations that understand the value of their knowledge would want their KM personnel to be able to protect it. It is expected that all KM managers should be familiar with organizational Information Security standards and policies. It is understandable if organizations were to create new KM technician positions focused on secure KM but this study found only one posting that fit this: Knowledge Management Secured Messaging Specialist. Since there were 11 postings focused on defense organizations it is surprising to note this specialist posting was for a commercial bank.[6]

We asked Murray about any practitioner feedback that he had received about his research and he responded:

> We are also going to be expanding on the article, in particular the survey and looking at how KM governance can incorporate security … I don't get a lot of response from the KM community on security. I figure it's just a matter of time before this becomes an issue with us. The response I do get is from the government KM people (defense in particular) so they are seeing problems now and it will hit the rest of us soon.[7]

However, the approach of cybersecurity professionals cannot be "business prevention", ie risks have to managed in constructive and commercial ways. The response of information professionals asks that cybersecurity professionals think through the implications of their actions.

Albert Simard (Knowledge Manager for Defense Research & Development Canada) commented:

> In my experience, cyber security is both essential and problematic. Sensitive internal content must be protected whereas knowledge workers must be able to connect with their external professional colleagues. This contradiction poses a dilemma that cannot be resolved in an absolute sense. The only absolutely secure network is one with an air gap between it and the outside world which certainly precludes external collaboration. Conversely, experience demonstrates that an isolated network becomes disassociated from and falls behind external events and progress. For the public sector, this results in reduced service to citizens whereas for the private sector, it eventually results in business failure.
>
> When a security breach occurs, the automatic, knee jerk reaction is to cut off all contact with the outside world. The security goal is to protect the network at any cost. If that means stopping work, so be it. However, professionals still have deadlines to meet and need to get their work done. So, they work and connect from home or even cyber cafes and bring content back and forth on memory sticks. I once asked a security guru which work process posed the greater security risk – passing content through sophisticated agency filters that bits can barely squeeze through or working from home and carrying content back and forth. He simply rolled his eyes!
>
> One solution is to have two separate networks – one only connected externally and another only connected internally. However, this requires a reasonable and secure process for transferring content from one network to the other. People will gravitate to the external network for general work because it will inevitably be more flexible, faster, and have better applications. A lot of convenient productivity applications cannot meet stringent security requirements. A process that strips all active code from content before it is transferred works well for this purpose.

[6] Jennex M and Durcikova A, "Integrating IS Security with Knowledge Management: Are We Doing Enough?" (2014) 10 *International Journal of Knowledge Management* 1 (available at http://dx.doi.org/10.4018/ijkm.2014040101).

[7] Jennex M, Personal Communication (2 April 2015).

> Neither total isolation nor total openness are appropriate in a complex and rapidly changing world. The challenge is to balance risks and security requirements. Anyone will accept reasonable and balanced security inconveniences. Problems occur when security requirements significantly exceed the perceived risk. It is essential to understand that the key perception is in the mind of knowledge workers – not the IT security professionals.[8]

A commenter who would rather remain anonymous stated:

> I work security on an operational level – I have servers to maintain, OpenSSL updates to install, etc. The people who work security purely on a bureaucratic level have two bad habits that make any type of sharing much more difficult: 1. Management by checklist: "If I get my spreadsheet just right, our systems will be secure." No, they won't. Checklists are an aid to people with experience, not a replacement for those people. 2. "Anything less than airtight security is unacceptable." Seldom right and wrong again; there's no such thing unless you want to unplug your network cable. It's getting to the point where the cost of protecting information is starting to exceed any value we might get from keeping it in the first place.

These comments highlight the importance of a holistic approach to information security. If the full impact of the proposed security solutions and the responses of staff to them are not considered, then the end result will be a less, not more, secure organisation. This may necessitate a review of what security means from a content perspective.

John Mancini, CEO of the Association for Information and Image Management (AIIM), says:

> We spend countless – albeit necessary – cycles worrying about perimeter and device security. That won't go away, but it is no longer enough. It's kind of like the fiction of relying on the Maginot Line to keep out the invaders. Once the invaders went mobile, the jig was up… We need to move from perimeter security and device-based security to security linked directly to the information asset itself. And 2015 is the year organizations will begin to seriously embrace this concept.[9]

This asset-based approach is actually useful to information professionals because it can force organisations to value the information they hold. Is it worth the security procedures being put in place around it? If not, then perhaps it should not be held. Of course, another trend is working in parallel to this. The mantra of "big data" is that all data should be held for as long as possible because it might yield useful insights at some point in the future. Exactly how these trends play out remains to be seen – observers have noted that Australia's privacy legislation is not keeping pace with these technological developments.

CONCLUSION

The growing importance of effective information security was recently highlighted as the number one issue in the AIIM's *Content Management 2020: Thinking Beyond ECM*: "The proportion of effort the enterprise has to spend on ensuring privacy and security will increase."[10]

Information security issues will only become more acute for organisations as their dependence on technology grows. The challenge for information professionals is to correctly prioritise security concerns within their broader remit of collection, connection and curation. This means that they have to work with security professionals to identify risks early. The risk identification process can even support the work of information professionals because it requires organisations to put a price on the information in question. Good information management practices are often good security practices – eg focusing on a single source of truth rather than multiple, duplicate repositories reduces the attack surface and vulnerability of that information as well as making it more reliable for users.

At the same time, there is an opportunity for information professionals to ground the work of security professionals in the practicalities of business. Risk is tied to reward and the optimal risk

[8] Simard A, Personal Communication (5 April 2015).

[9] Mancini J, "2015 Prediction No 5 – Security Shifts from the Perimeter and the Device to the Asset Itself", *Association of Information and Image Management* (21 December 2014) http://info.aiim.org/digital-landfill/2015-predictions-security-shifts-from-the-perimeter-and-the-device-to-the-asset-itself.

[10] Association for Information and Image Management, *Content Management 2020: Thinking Beyond ECM* (2015) http://www.aiim.org/Research-and-Publications/Research/AIIM-White-Papers/ELC-ContentManagement2020.

profile for every organisation is not zero. Given that people are often the most vulnerable point of a system, understanding the vagaries of human nature is key to making security effective.

Ultimately, we all want our lives to be enriched by information technology – and we want to be as safe as we can in the process.